**REMARKS**

This Amendment is in response to the Final Office Action dated July 9, 2008 ("FOA"). In the Final Office Action, claims 30-38 were rejected under 35 U.S.C. § 103. By this Amendment, claim 30 is amended and claims 39-47 are added. Currently pending claims 30-47 are believed allowable, with claim 30 and 39 being independent claims.

CLAIM REJECTIONS UNDER 35 USC §103:

Claims 30-36 and 38 were rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,834,350 to Boroughs et al. ("Boroughs") in view of U.S. Patent No. 6,971,026 to Fujiyama et al. ("Fujiyama"). FOA, pp. 2.

The Applicants respectfully note that while page 2 of the Final Office Action alleges that claims 30-38 are rejected as unpatentable over Boroughs in view of Fujiyama, claim 37 is not discussed in the subsequent arguments.

Claim 37 was rejected under 35 U.S.C. § 103 as unpatentable over Boroughs in view of Fujiyama and further in view of U.S. Patent No. 6,990,591 to Pearson ("Pearson"). FOA, pp. 4.

Claim 30

A. "the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information."

Claim 30 recites, in part, "the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information."

In rejecting claim 30 as presented in the Amendment filed April 30, 2008, the Examiner alleges that column 2, line 59 through column 3, line 10 of Boroughs teaches "a first system configured to at least review security and vulnerability information form [sic] information publishers and to provide the activation token based on the security and vulnerability information." FOA, pp. 2. The cited passage recites,

> Distributions are preferably prepared by a team of network security experts. A distribution may contain information, such as textual information, for review by a network security administrator. For example, the distribution could contain information describing a newly-discovered form of network attack, and explain how network security equipment or software already being used by the subscriber protects the subscriber from such attacks. A distribution may also contain software. Such software can include both software designed to execute once to ensure that the subscriber's network is protected from a certain type of attack, or new or updated network security software that executes continuously to ensure the security of the subscriber's network. A distribution may also contain data used for network security purposes. For example, where a subscriber uses a particular network security device that operates based upon a set of security rules, a distribution to the subscriber may contain additional rules to be added to the set used by the network security device. Boroughs, col. 2, ll. 59 through col. 3, ll. 10.

The Applicants respectfully submit that the passage cited by the Examiner fails to recite any specific steps performed by the team of network security experts to prepare the distributions. Therefore, the cited passage fails to provide

sufficient information to enable one of ordinary skill in the art to reconstruct the operations by which the distributions are prepared. Because the cited passage fails to provide an enabling disclosure of preparing the distributions, the preparation of the distributions cannot teach the first system of claim 30.

B. "a second system configured to receive the activation token from a source external to the second system."

By this Amendment, claim 30 is amended to recite, in part, "a second system configured to receive the activation token from a source external to the second system."

Support for the limitation requiring that the second system is configured to receive the activation token is found in at least page 4, lines 26-27 (paragraph [0007]) of the specification, which states, "The second subsystem comprises receiving means for controlling the receiving of activation tokens . . . ." Further support is found in page 11, lines 10-13 (paragraph [0027]) of the specification, which states,

> The embodiment according to the FIG. 1 shows a second subsystem 2 with an apoptosis system 9 and at least one service 10 run by the customer on the second subsystem 2. The apoptosis system 9 is preferably built into a daemon of the second subsystem 2 and comprises receiving means 11 for receiving activation tokens . . . .

Support for the limitation requiring that the activation token is received from a source external to the second system is found in at least page 4, lines 23-24 (paragraph [0007]) of the specification, which states, ". . . wherein a service provider

with a first subsystem is providing activation tokens to be received by a customer with a second subsystem." Furthermore, Figure 1 clearly shows that the first subsystem (item 1) is distinct from the second subsystem (item 2.) Therefore, the first subsystem is external to the second subsystem. It follows that when activation tokens provided by the first subsystem are received at the second subsystem, the activation tokens are received from a source external to the second subsystem.

In rejecting claim 30 as presented in the Amendment filed April 30, 2008, the Examiner alleges that column 3, lines 35-67 and column 4, lines 1-5 of Boroughs teach "a second system configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system the activation measure configured to modify services executing at the second system." FOA, pp. 2-3. The cited passage recites,

> After the distribution is addressed to addressees among the registered subscribers, the facility attempts to deliver the distribution to each of the addressees to which the distribution is addressed. The facility may preferably deliver distributions either by secure email sent from the network security information service to the addressees, or using a client polling procedure in which a client program at each subscriber periodically polls a server maintained by the network security information service for new distributions addressed to its subscriber. In order to implement the client polling procedure, in certain embodiments, the facility utilizes BackWeb Foundation software, available from BackWeb Technologies of San Jose, Calif. For emailed distributions, a verified email address

> for the subscriber is preferably used. For distributions delivered by the client polling procedure, polling requests from the client preferably include a secret unique identifier issued to the subscriber, encrypted using public key encryption. These measures help ensure that the distribution is delivered only to the subscribers to which it is addressed.
>
> During delivery, each distribution is preferably encrypted to prevent anyone intercepting the distribution from discerning its content. Each distribution is preferably also signed in way that reliably indicates both (1) the source of the distribution, and (2) the contents of the distribution when the distribution left its source. This signature is preferably used by a component of the facility executing at each subscriber to ascertain whether each distribution (1) is from the network security information service or another trusted source and (2) has not been altered since it left that source. The subscriber component of the facility preferably only allows the subscriber to make use of distributions meeting both of these conditions.
>
> The client program of the facility preferably also alerts a user at the subscriber as soon as a distribution is received, displays information about the distribution, and facilitates the application of the distribution to enhance the level of security of the subscriber's network. Boroughs, col. 3, ll. 35 through col. 4, ll. 5.

In the Response to Arguments section, the Examiner further alleges,

> . . . in column 3 lines 35-67 and column 4 lines 1-5 Boroughs describes a system that has a facility and subscribers, these entities combine to form the "second system" of claim 30. Therefore, the facility determines which distributions are useful to each subscriber and sends them to each subscriber who then facilitates the application of the distribution (i.e. transforming the activation token to modify services of the second system).

> Therefore, Boroughs teaches the second system of claim 30. FOA, pp. 6-7.

Thus, the Examiner alleges that the facility and subscribers combine to form the second system required by claim 30. The Examiner further alleges that the facility sends distributions to each subscriber.

However, claim 30 as currently presented recites, in part, "a second system configured to receive the activation token from a source external to the second system." If the facility is included in the second system, then a distribution sent by the facility is clearly not received from a source external to the second system. Therefore, the Applicants respectfully submit that even assuming *arguendo* that the distribution of Boroughs is equivalent to the activation token of claim 30, the combined facility and subscribers cannot teach the second system of claim 30.

C. "the second system further configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system, the activation measure configured to modify services executing at the second system."

By this Amendment, claim 30 is amended to recite, in part, "the second system further configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system, the activation measure configured to modify services executing at the second system."

Thus, claim 30 requires a second system configured to determine whether the activation token is relevant. Moreover, it is evident from antecedent basis that this second system is the same second system at which the activation measure is configured to modify executing services. Therefore, Boroughs cannot teach claim 30 unless the activation measure is configured to modify services executing at the same system which is configured to determine whether the activation token is relevant.

As noted above in regards to subheading (B), in rejecting claim 30 as presented in the Amendment filed April 30, 2008, the Examiner alleges that column 3, lines 35-67 and column 4, lines 1-5 of Boroughs teach "a second system configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system the activation measure configured to modify services executing at the second system."

FOA, pp. 2-3. The cited passage is reproduced above in regards to subheading (B).

In a passage preceding the above passage, Boroughs states, "The present invention provides a software facility for the secure and differentiated delivery of network security information ('the facility') to support a network security information service." Boroughs, col. 2, ll. 48-51. Thus, it is evident that "the facility", as the term is used by Boroughs, is a software facility for the delivery of network security information.

The final sentence of the passage cited by the Examiner teaches that the facility facilitates the application of the distribution to enhance the level of security of the subscriber's network. The facility is clearly not equivalent to the subscriber's network. It follows that the facility is not equivalent to the system to which the distribution is applied.

As previously noted, claim 30 requires a second system configured to determine whether the activation token is relevant. The Applicants respectfully submit that the passage cited by the Examiner is devoid of any discussion of determining whether the activation token is relevant. Therefore, the passage cited by the Examiner cannot, by itself, teach the second system of claim 30.

The paragraph immediately preceding the passage cited by the Examiner recites,

> Because some distributions are only useful to subscribers having certain security characteristics, such as those having a particular network security device, the facility preferably selects addressees for each distribution from the subscribers registered with the network security

> information service. In this regard, the facility preferably uses a subscriber information database that stores information about each subscriber registered with the network security information service. For example, the subscriber database may contain, for each subscriber, an indication of the types of network security equipment, network security software, and applications used by the subscriber. When the facility receives a new distribution, it preferably receives with it an addressing query designed to select addressees for the distribution. The facility performs the addressing query against the subscriber information database to select addressees of the distribution. By selecting addressees for a distribution (or "addressing" the distribution), the facility maximizes the extent to which each registered subscriber receives the distributions that relate to it, and minimizes the extent to which each registered subscriber receives distributions that do not relate to it. Also, by directly controlling the set of addressees, the facility ensures that distributions are not delivered to parties other than subscribers. Boroughs, col. 3, ll. 11-34.

This passage discloses that the facility performs the addressing query against the subscriber information database to select addressees of the distribution. However, as previously noted, the facility is not equivalent to the system to which the distribution is applied. Moreover, as previously noted, claim 30 requires that the activation measure is configured to modify services executing at the same system which is configured to determine whether the activation token is relevant. Therefore, even assuming *arguendo* that the distribution is equivalent to an activation token, that the steps performed by the facility are equivalent to determining whether the distribution is relevant, and that the distribution is configured to modify services executing at the system to which it is applied, the facility nonetheless fails to teach the second system of claim 30. This

is evident because even in this case, the facility would not modify services executing at itself.

Furthermore, for the reasons discussed above, the case wherein the combined facility and subscribers are equivalent to the second system of claim 30 fails to fulfill the limitation of subheading (B) of claim 30. Therefore, the question of whether the case wherein the combined facility and subscribers are equivalent to the second system of claim 30 fulfills the limitation of subheading (C) of claim 30 is moot.

Moreover, Figure 17 of Boroughs discloses a flowchart of steps performed by the subscriber. Figure 17 shows that if a distribution is received at step 1706, the distribution is always processed. The only possible exception is if the security check at step 1710 finds that one-way function results failed to match. However, this is an exception condition which should only occur if the distribution is corrupt or unauthorized. Specifically, the security check at step 1710 is clearly not equivalent to a determination whether the distribution is relevant. Thus, Figure 17 teaches that the system to which the distribution is being applied does not make a determination whether the distribution is relevant. This teaches away from an activation measure configured to modify services executing at the same system which is configured to determine whether the activation token is relevant as required by claim 30.

D. "wherein the first system is further configured to automatically filter the security and vulnerability

information relevant to the system characteristics identified by the activation token."

The Examiner further states, "wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token (see column 2 line 59 through column 3 line 10 and Figure 17)." FOA, pp. 3.

The Applicants respectfully submit that claim 30 does not recite the limitation of subheading (D). Instead, the limitation of subheading (D) is recited in claim 33. Thus, the question of whether Boroughs teaches the limitation of subheading (D) is not relevant to the question of whether claim 30 is allowable.

E. Motivation to reconstruct Boroughs in light of Fujiyama

The Examiner further argues that ". . . it would have been obvious to a person of ordinary skill in the art to include trust levels with the activation tokens of Boroughs et al. Motivation to do so would have been to distinguish between the types of threats (see figures 2-5 and column 7 line 54 through column 8 line 55)." FOA, pp. 3.

The Applicants respectfully submit that neither claim 30 nor Fujiyama recites "trust levels". Instead, Fujiyama shows a "security level" in Figures 2-5. Nonetheless, Boroughs fails to express any appreciation of the benefits of distinguishing between different types or levels of security threats. To the contrary, as discussed above, Figure 17 of Boroughs teaches that

the system receiving a distribution always processes the distribution unless the distribution fails a security check. This teaches away from a system which processes distributions selectively based on the type or level of threat which the distribution concerns. For this reason, one would not be motivated to reconstruct Boroughs in light of Fujiyama to create a system which includes the security levels disclosed by Fujiyama in activation tokens in order to distinguish between different types of threats.

In responding to this argument, the Examiner alleges,

> . . . the fact that Boroughs teaches always installing the distribution does not teach away from the selective installation of Fujiyama. Boroughs already teaches selectively installing certain distributions based on system characteristics, therefore it would be obvious to one of ordinary skill in the art to add the further selection based on security level as taught by Fujiyama in order to distinguish between types of threats. Therefore, Boroughs does not teach away from the combination and the combination is proper. FOA, pp. 7.

The Applicants respectfully submit that whether or not a distribution is relevant to a given system, based on the characteristics of the system, is qualitatively different from the severity of the threat addressed by the distribution. Therefore, it would not be obvious, given a teaching of selective installation based on system characteristics, to selectively install based on the severity of a threat. Accordingly, it would not be obvious, based on a teaching of selective installation based on system characteristics, to selectively install based on a level expressing the severity of a threat.

Similarly, whether or not a distribution is relevant to a given system, based on the characteristics of the system, is qualitatively different from the type of the threat addressed by the distribution. Therefore, it would not be obvious, given a teaching of selective installation based on system characteristics, to selectively install based on the type of a threat.

It follows that the teaching of Figure 17 of Boroughs that the system receiving a distribution always processes the distribution unless the distribution fails a security check, as discussed above, in fact teaches away from combining Boroughs and Fujiyama.

For at least these reasons, claim 30 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 30.

Claim 31

Claim 31 is dependent on and further limits claim 30. Since claim 30 is believed allowable, claim 31 is also believed allowable for at least the same reasons as claim 30.

Claim 32

Claim 32 recites, "The system of claim 30, further comprising a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system." Thus, claim 32 requires not only a report to a system administrator but additionally requires that

the report comprises any activation measures taken by the second system.

Moreover, claim 30 recites, "the second system further configured to transform the activation token into at least one activation measure." Thus, an activation measure, as the term is used in claim 32, is clearly required to be a result of a transformation of an activation token.

The Examiner alleges that "the modified Boroughs et al. and Fujiyama et al. system" teaches the limitation introduced by claim 32. FOA, pp. 3-4. In support of this position, the Examiner cites column 2, lines 59-67 of Boroughs. FOA, pp. 4. The passage cited by the Examiner states,

> Distributions are preferably prepared by a team of network security experts. A distribution may contain information, such as textual information, for review by a network security administrator. For example, the distribution could contain information describing a newly-discovered form of network attack, and explain how network security equipment or software already being used by the subscriber protects the subscriber from such attacks. A distribution may also contain software. Such software can . . . . Boroughs, col. 2, ll. 59-67.

The cited passage of Boroughs discloses information being reviewed by a network security administrator. The passage discloses that a distribution may contain information for review by a network security administrator. However, the Examiner has not explained, and it is not apparent, how such information is equivalent to activation measures taken by the second system. The passage further discloses that the information may be "textual information" or "information describing a newly-discovered form of network attack." However, neither of these

types of information is equivalent to a report to a system administrator of activation measures.

The passage additionally discloses that a distribution may contain "software." Furthermore, immediately following the cited passage at column 3, line 5, Boroughs discloses that the distribution may contain "data." (It is noted that the passage of Boroughs from column 2, line 59 through column 3, line 10 is reproduced above in regards to subheading (A).) However, neither software nor data is equivalent to a report to a system administrator of activation measures.

The cited passage further outlines an example wherein the distribution explains "how network security equipment or software already being used by the subscriber protects the subscriber from such attacks." However, as previously noted, claim 32 requires that an activation measure results from the transformation of an activation token. It is apparent from the words, ". . . already being used . . .", that the network security equipment or software was already employed prior to receiving the distribution. It follows that the network security equipment or software is clearly not a result of a transformation of the exemplary distribution. Therefore, even assuming *arguendo* that the exemplary distribution is equivalent to an activation token, the network security equipment or software cannot be equivalent to an activation measure. Accordingly, the Applicants respectfully submit that the example disclosed in the passage cited by the Examiner fails to teach a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system as required by claim 32.

Therefore, the Applicants respectfully submit that the cited passage of Boroughs and the distributions disclosed therein fail to teach or suggest a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system as required by claim 32.

In responding to the argument outlined above, the Examiner alleges, "Boroughs discloses alerting a user based on the received distribution (see column 4 lines 1-5) . . . ." FOA, pp. 7. The passage of Boroughs cited by the Examiner states,

> The client program of the facility preferably also alerts a user at the subscriber as soon as a distribution is received, displays information about the distribution, and facilitates the application of the distribution to enhance the level of security of the subscriber's network. Boroughs, col. 4, ll. 1-5.

As previously noted, an activation measure, as the term is used in claim 32, is clearly required to be a result of a transformation of an activation token. The cited passage of Boroughs recites alerting a user as soon as a distribution is received. The Applicants respectfully submit that the mere receiving of a distribution is not equivalent to the transformation of a distribution. Similarly, the mere receiving of a distribution is not equivalent to a result of a transformation of a distribution. Therefore, even assuming *arguendo* that the distribution is equivalent to an activation token, receiving a distribution is clearly not equivalent to an activation measure as the term is used in claim 32. Therefore, alerting a user as soon as a distribution is received cannot teach or suggest a reporting means configured to report to a

system administrator of the second system any activation measures taken by the second system as required by claim 32.

The Examiner further alleges, ". . . and further as shown in column 2 lines 56-67 the user can be an administrator." FOA, pp. 7.

The Applicants respectfully submit that the reasons outlined above as to why the passages of Boroughs cited by the Examiner fail to teach or suggest the limitations of claim 32 hold regardless of whether or not the user is a system administrator. Therefore, the question of whether the user can be an administrator is moot.

For at least these reasons, claim 32 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 32.

Claims 33-38

Claims 33-38 are dependent on and further limit claim 30. Since claim 30 is believed allowable, claims 33-38 are also believed allowable for at least the same reasons as claim 30.

NEW CLAIMS:

Claim 39

By this Amendment, claim 39 is added. Claim 39 recites the subject matter of claim 30 as presented in the Amendment filed April 30, 2008.

Claim 39 further includes an additional limitation which recites, "wherein the information publishers are external to the

first system." Support for the limitation requiring that the information publishers are external to the first system is found in at least Figure 1, which clearly shows that the first subsystem (item 1) is distinct from the information publishers (item 3.) Therefore, the information publishers of Figure 1 are external to the first subsystem of Figure 1.

Because claim 39 as currently presented recites the subject matter of claim 30 as presented in the Amendment filed April 30, 2008, the Examiner's arguments regarding claim 30 are addressed in regards to claim 39 as currently presented.

A. "the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information, wherein the information publishers are external to the first system."

Claim 39 recites, in part, "the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information, wherein the information publishers are external to the first system."

In rejecting claim 30 as presented in the Amendment filed April 30, 2008, the Examiner alleges that column 2, line 59 through column 3, line 10 of Boroughs teaches "a first system configured to at least review security and vulnerability information form [sic] information publishers and to provide the

activation token based on the security and vulnerability information." FOA, pp. 2. The cited passage recites,

> Distributions are preferably prepared by a team of network security experts. A distribution may contain information, such as textual information, for review by a network security administrator. For example, the distribution could contain information describing a newly-discovered form of network attack, and explain how network security equipment or software already being used by the subscriber protects the subscriber from such attacks. A distribution may also contain software. Such software can include both software designed to execute once to ensure that the subscriber's network is protected from a certain type of attack, or new or updated network security software that executes continuously to ensure the security of the subscriber's network. A distribution may also contain data used for network security purposes. For example, where a subscriber uses a particular network security device that operates based upon a set of security rules, a distribution to the subscriber may contain additional rules to be added to the set used by the network security device. Boroughs, col. 2, ll. 59 through col. 3, ll. 10.

The Applicants respectfully submit that the cited passage fails to teach or suggest a first system configured to at least review security and vulnerability information from information publishers, wherein the information publishers are external to the first system.

Moreover, the passage cited by the Examiner fails to recite any specific steps performed by the team of network security experts to prepare the distributions. Therefore, the cited passage fails to provide sufficient information to enable one of ordinary skill in the art to reconstruct the operations by which the distributions are prepared. Because the cited passage fails to provide an enabling disclosure of preparing the

distributions, the preparation of the distributions cannot teach the first system of claim 39.

Furthermore, the network security administrator disclosed by Boroughs clearly does not receive the distribution until after the distribution is prepared. Actions on which preparing a distribution as disclosed by Boroughs is based must occur before the distribution is prepared. Therefore, it is impossible for the distribution to be provided based on any action taken by the network security administrator. Thus, even though Boroughs suggests that the network security administrator reviews distributions, such a review by the network security administrator cannot teach or suggest providing an activation token based on reviewed security and vulnerability information as required by claim 39.

The remainder of the passage cited by the Examiner discloses content which a distribution may contain. Such content includes "information", "software" and "data". Information and data are clearly not equivalent to a first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information. Moreover, Boroughs does not disclose that the software is configured to review security and vulnerability information. Nor does Boroughs disclose that the software is configured to provide an activation token based on the security and vulnerability information. It follows that the software disclosed by Boroughs is not equivalent to the first system of claim 39.

The Examiner further alleges,

> With respect to Applicant's argument that Boroughs fails to disclose "a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on filtered security and vulnerability information", in column 2 lines 59-67 Boroughs describes a distribution (i.e. activation token). These distributions are prepared by network security experts and contain information describing newly-discovered network attacks (i.e. security and vulnerability information). This information can be obtained in one of two ways, either the experts find the attack themselves or receive information from one or more other entities. In the first case the experts themselves are the "information publishers" otherwise the other entities are the information publishers. FOA, pp. 6.

The passage cited by the Examiner in the argument reproduced above is a subset of the passage of Boroughs reproduced above. The Applicants respectfully submit that this passage is silent as to whether the network security experts find the attack themselves or receive information from one or more other entities.

Moreover, the Examiner concedes that the experts may find the attack themselves. The Examiner further concedes that in this case, the experts themselves are the "information publishers." In this case, the information publishers are clearly not external to a system comprising the experts. Therefore, the cited passage does not inherently disclose that the experts review security and vulnerability information from information publishers, wherein the information publishers are external to a system comprising the experts. It follows that even if a first system comprises the experts disclosed by Boroughs, and even assuming *arguendo* that the distribution of Boroughs is equivalent to the activation token of claim 39, the

cited passage fails to teach or suggest that the first system reviews security and vulnerability information from information publishers, wherein the information publishers are external to the first system, as required by claim 39.

B. Motivation to reconstruct Boroughs in light of Fujiyama

The Applicants respectfully submit that the reasons provided above in regards to subheading (E) of claim 30 as to why one would not be motivated to reconstruct Boroughs in light of Fujiyama apply equally to claim 39.

For at least these reasons, claim 39 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 39.

Claim 40

By this Amendment, claim 40 is added.

Claim 40 is dependent on and further limits claim 39. Since claim 39 is believed allowable, claim 40 is also believed allowable for at least the same reasons as claim 39.

Claim 41

By this Amendment, claim 41 is added.

Claim 41 introduces limitations which are substantially similar to the limitations introduced by claim 32. Therefore,

claim 41 is believed allowable for at least the same reasons as claim 32.

Moreover, claim 41 is dependent on and further limits claim 39. Since claim 39 is believed allowable, claim 41 is also believed allowable for at least the same reasons as claim 39.

It is noted that the argument outlined above for claim 32 depends on the fact that claim 32 is dependent on claim 30 and that claim 30 recites, "the second system further configured to transform the activation token into at least one activation measure." However, claim 41 is dependent on claim 39, and this limitation is also found in claim 39.

Claims 42-47

By this Amendment, claims 42-47 are added.

Claims 42-47 are dependent on and further limit claim 39. Since claim 39 is believed allowable, claims 42-47 are also believed allowable for at least the same reasons as claim 39.

**CONCLUSION**

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue that the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

No fee is believed due with this Amendment, however, should such a fee be required please charge Deposit Account 50-0510 the

required fee. Should any extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: October 9, 2008

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (718) 374-6092